CLAIMS

What is claimed is:

1. A method comprising:

registering a first biometric data with a trusted entity;

sensing a second biometric data;

comparing the second biometric data to the first biometric data; and

preventing the registration of the second biometric data at the trusted entity as associated with an authorized user if the second biometric data does not match the first biometric data.

2. The method of claim 1, further comprising:

storing a copy of the first biometric data on a transaction device.

3. The method of claim 1, further comprising:

notifying in real-time one of a security entity and the authorized user of an unauthorized attempt to register the second biometric data.

4. The method of claim 1, further comprising:

accessing a financial account associated with the first biometric data if the first biometric data matches the second biometric data; and

transferring funds in real-time to a supplier.

5. The method of claim 4, further comprising:

withholding identifying information associated with the first biometric data from the supplier.

6. The method of claim 1, further comprising:

earmarking assets associated with the first biometric data and transferring the assets of the account in real-time to pay for one of a product and a service.

7. An article comprising:

a storage medium at a trusted entity including instructions stored thereon which when executed cause a digital system to perform a method including:

registering a first biometric data of a user with the trusted entity;

sensing a second biometric data from a person;

comparing the second biometric data to the first biometric data; and

preventing the person from registering the second biometric data at the trusted entity as associated with the user if the second biometric data does not match the first biometric data.

8. The article of claim 7, wherein the method further includes:

storing a copy of the first biometric data on a transaction device.

9. The article of claim 7, wherein the method further includes:

storing a copy of the first biometric data on one of a privacy card, a digital wallet, and a privacy card configured to be coupled to a digital wallet.

10. The article of claim 7, wherein the method further includes:

notifying in real-time one of a security entity and the user of an unauthorized attempt to register the second biometric data.

11. The article of claim 7, wherein the method further includes:

accessing a financial account of the person provided that the first biometric data matches the second biometric data; and

transferring funds in real-time to a supplier.

12. The article of claim 7, wherein the method further includes:

withholding an identification of the person from the supplier.

13. The article of claim 7, wherein the method further includes:

performing one of earmarking assets of the user and transferring assets of the account in real-time to pay for one of a product and a service.

14. A method of performing an electronic transaction using a transaction device comprising:

registering a first biometric data with a trusted entity in which the first biometric data is associated with a user;

storing a copy of the first biometric data on the transaction device;

providing the transaction device to the user;

sensing a second biometric data from a person;

comparing the second biometric data to the first biometric data stored on the transaction device;

authenticating the transaction provided that the second biometric data matches the first biometric data;

performing one of earmarking assets of the user and transferring assets of the account in real-time to pay for one of a product and a service; and

authorizing the electronic transaction.

15. The method of claim 14, further comprising:

notifying in real-time one of a security entity and the user of an unauthorized attempt to access financial credit of the user.

16. The method of claim 14, further comprising:

withholding an identification of the user from the supplier.

17. A system for preventing a person from improperly obtaining financial credit comprising:

a recording medium of a trusted entity configured to register a first biometric data of a user;

a processor, coupled to the recording medium, configured to store the first biometric data onto a transaction device and to prevent registration of a second biometric data that fails to match the first biometric data;

the transaction device comprising a chip configured to store the first biometric data and a sensor to sense the second biometric data from the person; and

means for preventing the person from improperly receiving financial credit if the person's second biometric data fails to match the first biometric data.

18. The system of claim 17, wherein the transaction device is selected from the group consisting of a privacy card, a digital wallet, and a privacy card configured to be coupled to a digital wallet.

19. The system of claim 17, wherein a party is electronically notified of an unauthorized use of the transaction device.

20. The system of claim 19, wherein the party is one of an owner of the transaction device and a security authority.

21. An electronic transaction device for use in a consumer purchasing system comprising:

a transaction device identifier providing no apparent identification of a user authorized to use the transaction device;

communication logic, disposed on a processor of the transaction device, configured to communicate the transaction device identifier to the system to perform a transaction, the system comprising a secure mechanism for correlating the device identifier and the user; and

security logic, disposed on a processor of the transaction device, configured to compare a registered first biometric data of an authorized user to a second biometric data read from a person attempting to use the transaction device.

22. The electronic transaction device of claim 21, wherein the transaction device is selected from the group consisting of a privacy card, a digital wallet, and a privacy card configured to be coupled to a digital wallet.

23. The electronic transaction device of claim 21, wherein the security logic that confirms an identification of an authorized user is selected from the group consisting of a PIN code and a fingerprint.

24. The electronic transaction device of claim 21, wherein the communication logic is selected from the group consisting of a smart card chip interface, contactless connection, magnetic stripe and wireless connection.